

REMARKS

In the Office Action, the Examiner rejected Claims 1-43, which are all of the pending claims, over the prior art, principally U.S. Patent 6,031,910 (Deindl, et al.). In particular, Claims 1, 2, 4, 11-15, 17, 19, 26-29, 35, 36, 41 and 42 were rejected under 35 U.S.C. §102 as being fully anticipated by Deindl, et al; and Claims 3, 5-10, 16, 18, 10-25, 30-34, 37-40 and 43 were rejected under 35 U.S.C. §103 as being obvious over Deindl, et al, in view of U.S. Patent 5,721,781 (Deo, et al.).

Independent Claims 1, 14, 28, 35 and 41 are being amended to improve the form of the claims and to emphasize the differences between the claims and the prior art.

The present invention, generally, relates to methods and systems for securely handling an information unit by a first processing device interacting with a second processing device. More specifically, the invention relates to such methods and systems where that information unit is sent by an issuer to the first processing device, for example, over the Internet. To achieve this secure handling, the second processing device is provided with a key that, in use, is transmitted to the first processing device and used by the latter device to decrypt or authenticate the information. In this way, even though the information unit may be sent over a public network, the user of the second device retains control over access to the information in that information unit.

Deindle, et al. discloses a procedure for protecting information on a card. The data on that card is encrypted, and the card also holds the key for decrypting that data. With this arrangement, the information on the card can be sent to a plurality of users, while only personnel authorized by the holder of the card are permitted to read that information.

There is an important general difference between the present invention and the method and system disclose in Deindl, et al. With this invention, the pertinent information unit is sent from the issuer to the first processing device, while in Deindle, et al, the information unit is sent from the card holder to the card reader. As a result of this difference, the present invention is much better suited for use with information that is sent over a public network.

This general difference between this invention and Deindl, et al. is reflected in a number of more specific differences between the preferred embodiment of the present invention and the disclosure of Deindl, et al. For instance, with this preferred embodiment, the first processing device, on the one hand, receives the information unit from the issuer, and, on the other hand, receives the key for decrypting or authenticating the information unit from the second processing device. In contrast, with Deindl, et al, both the information and the decryption key are sent from the card to the card reader.

Independent Claims 1, 14, 28, 35 and 41 are being amended to describe the above-discussed feature of this invention. In particular, Claims 1 and 41 are being amended to indicate positively that the information unit is transmitted from the issuer to the first processing device, and that this processing device receives the key from the second processing unit and uses that key to cryptographically reprocess the information unit. Claim 14, which is directed to a system for securely handling an information unit, is being amended to include analogous apparatus limitations.

Claim 28 is directed to a chip card for securely handling an information unit by interoperating with an information handling terminal device. This claims is being amended to include the limitation of means for transmitting at least one key to that handling device, to enable

that device to cryptographically process an information unit received by that device from an issuer. Claim 35, which is directed to a chip card accepting device, is being amended herein to add the limitations of means for receiving at least one key from a chip card, and means for cryptographically reprocessing the information unit by using that at least one key.

The above-discussed feature of the invention is of significant utility because it makes the invention very well suited for securely processing sensitive information transmitted over a public network.

The other references of record have been reviewed, and it is believed that these other references, whether they are considered individually or in combination, fail to teach the principle of sending the information unit to the first processing device from the issuer, while sending the key for authenticating or decrypting that information unit to the first processing device from the second processing device. For example, Deo, et al was cited for its disclosure of the use of a signature to authenticate a transmission message. This reference does not teach, however, modifying Deindl, et al. to include the above discussed feature that enables the secure handling of information units received from the issuer.

Because of the above-discussed differences between Claims 1, 14 and 35, and because of the advantages associated with those differences, these claims patentably distinguish over the prior art and are allowable. Claims 2-13 are dependent from Claim 1 and are allowable therewith; and Claims 15-27 are dependent from, and are allowable with, Claim 14. Likewise, Claims 29-34 are dependent from Claim 28 and are allowable therewith; Claims 36-40 are dependent from, and are allowable with, Claim 35; and Claims 42 and 43 are dependent from Claim 41 and are allowable therewith.

The Examiner is, accordingly, respectfully requested to reconsider and to withdraw the rejection of Claims 1, 2, 4, 11-15, 17, 19, 26-29, 35, 36, 41 and 42 under 35 U.S.C. §102, to reconsider and to withdraw the rejection of Claims 3, 5-10, 16, 18, 20-25, 30-34, 37-40 and 43 under 35 U.S.C. §103, and to allow Claims 1-43.

Every effort has been made to place this application in condition for allowance, a notice of which is requested. If the Examiner believes that a telephone conference with Applicants' Attorneys would be advantageous to the disposition of this case, the Examiner is asked to telephone the undersigned.

Respectfully submitted,

John S. Sensny
John S. Sensny
Registration No. 28,757
Attorney for Applicants

SCULLY, SCOTT, MURPHY & PRESSER
400 Garden City Plaza
Garden City, New York 11530
(516) 742-4343

JSS:jy

RECEIVED
CENTRAL FAX CENTER

OCT 22 2003

OFFICIAL